Aula 12

HOMOMORFISMO DE ANÉIS

META

Estabelecer o conceito de Homomorfismo de Anéis.

OBJETIVOS

Reconhecer e classificar homomorfismos de anéis.

Aplicar as propriedades básicas dos homomorfismos na resolução de problemas.

Aplicar o primeiro teorema dos isomorfismos.

PRÉ – REQUISITOS

As aulas 6, 10 e 11.

INTRODUÇÃO

Nesta aula, caro aluno, continuaremos o estudo dos homomorfismos que começamos na aula 6, onde lá os domínios e contradomínios eram grupos, aqui são anéis. É importante neste momento que você reveja a aula 6.

Como já dissemos anteriormente, os homomorfismos são aplicações que servem para comparar estruturas algébricas de mesma natureza. Os termos aqui usados são basicamente os mesmos que usamos para grupos. Temos núcleo e imagem de homomorfismo, os três teoremas de isomorfismos, etc.

O CONCEITO

Definição 1. Sejam A e A' anéis e ψ uma aplicação de A em A'. Dizemos que ψ é um homomorfismo se $\psi(a+b) = \psi(a) + \psi(b)$ e $\psi(a \cdot b) = \psi(a) \cdot \psi(b), \forall a, b \in A$.

Exemplo 1. Sejam A e A' anéis a aplicação nula $\psi: A \longrightarrow A', \psi(a) = 0, \forall a \in A$ é um homomorfismo de anéis. Notemos que $\psi(a+b) = 0 = 0 + 0 = \psi(a) + \psi(b)$ e $\psi(a \cdot b) = 0 = 0 \cdot 0 = \psi(a) \cdot \psi(b), \forall a, b \in A$.

Exemplo 2. Seja A um anel. A identidade de A é um homomorfismo de A em A. De fato, para $a, b \in A, I_A(a+b) = a + b = I_A(a) + I_A(b)$ e $I_A(a \cdot b) = a \cdot b = I_A(a) \cdot I_A(b)$.

Exemplo 3. Sejam A um anel e I um ideal. Seja $\psi: A \longrightarrow A/I$ dada por $\psi(a) = a + I$. Claramente ψ é um homomorfismo de anéis. Sejam $a, b \in A$ então $\psi(a+b) = (a+I) + (b+I) = \psi(a) + \psi(b)$ e, $\psi(a \cdot b) = a \cdot b + I = (a+I) \cdot (b+I) = \psi(a) \cdot \psi(b)$. Chamamos este homomorfismo ou projeção canônica de A sobre A/I.

A um homomorfismo de um anel A nele próprio chamamos um endomorfismo de A.

A um homomorfismo $\psi: A \longrightarrow A'$ injetivo, chamamos monomorfismo de A em A'.

A um homomorfismo $\psi: A \longrightarrow A'$ bijetivo, chamamos isomorfismo de A em A'. Neste caso dizemos que A e A' são anéis isomorfos.

A um isomorfismo de um anel A nele próprio, chamamos um automorfismo de A.

Proposição 1. Sejam A e A' anéis e $\psi: A \longrightarrow A'$ um homomorfismo. Então:

i) $\psi(0) = 0$

ii) $\psi(-a) = -\psi(a) \; \forall a \in A$.

iii) Se A e A' são domínios então ψ é a aplicação nula ou $\psi(1) = 1$.

Demonstração.

i) $\psi(0) = \psi(0+0) = \psi(0) + \psi(0) \Longrightarrow \psi(0) = 0$.
ii) $\forall a \in A, 0 = \psi(0) = \psi\big(a + (-a)\big) = \psi(a) + \psi(-a) \Longrightarrow \psi(-a) = -\psi(a)$.
iii) $\psi(1) = \psi(1 \cdot 1) = \psi(1)^2 \Longrightarrow \psi(1)(\psi(1) - 1) = 0 \Longrightarrow \psi(1) = 0$, ou $\psi(1) = 1$.
Exemplo 4. O único automorfismo de $\mathbb{Z}$ é o homomorfismo identidade. De fato, seja $\psi: \mathbb{Z} \longrightarrow \mathbb{Z}$ um automorfismo. Então, como $\mathbb{Z}$ é um domínio $\psi(1) = 1$. Assumindo por indução, que para $a > 1, \psi(a) = a, \psi(a+1) = \psi(a) + \psi(1) = a + 1$. Logo $\psi(a) = a, \forall a \in \{0,1,2,\dots\}$.

Finalmente, $0 = \psi(-1+1) = \psi(-1) + \psi(1) = \psi(-1) + 1 \Longrightarrow \psi(-1) = 1$. Segue que $\forall a > 0, \psi(-a) = \psi(-1) \cdot \psi(a) = -1 \cdot a = -a$.

Portanto, $\psi(a) = a, \forall a \in \mathbb{Z}$, ou seja, $\psi = I_{\mathbb{Z}}$.

Definição 3. Seja $\psi: A \longrightarrow A'$ um homomorfismo de anéis. Definimos o núcleo de ψ como sendo o conjunto $Ker\, \psi = \{a \in A;\ \psi(a) = 0\}$.
Proposição 2. Seja $\psi: A \longrightarrow A'$ um homomorfismo de anéis. Então, $Ker\, \psi$ é um ideal de A e $Im\, \psi$ é um subanel de A'.

Demonstração. Como $\psi(0) = 0 \Longrightarrow 0 \in Ker\, \psi$ e $Ker\, \psi \neq 0$. Sejam $a, b \in Ker\, \psi$. Então $\psi(a - b) = \psi(a) - \psi(b) = 0 - 0 = 0 \Longrightarrow a - b \in Ker\, \psi$.

Sejam $a \in A$ e $b \in Ker\, \psi$. Então, $\psi(a \cdot b) = \psi(a) \cdot \psi(b) = \psi(a) \cdot 0 = 0$. Ou seja, $a \cdot b \in Ker\, \psi$. Portanto $Ker\, \psi$ é um ideal de A.

Agora, de $\psi(0) = 0 \in Im\, \psi$ e se $a', b' \in Im\, \psi$, existem $a, b \in A$, tais que () = ′ e () = ′. Segue que (−) = () − () = ′ − ′ ∈ e que (·) = () · () = ′ · ′ ∈ . Portanto, é um subanel de ′.

Proposição 3. Seja : ⟶ ′ um homomorfismo de anéis. Então, é injetiva se, e somente se, = $\{0\}$.

Demonstração. Se ψ é injetiva, como $\psi(0) = 0$ segue que $Ker\, \psi = \{0\}$. Se $Ker\, \psi = \{0\}$ e $\psi(a) = \psi(b)$ então $\psi(a - b) = 0 \Longrightarrow a - b \in Ker\, \psi = \{0\} \Longrightarrow a = b$, ou seja, ψ é injetiva.

ISOMORFISMOS CANÔNICOS E O TEOREMA DA CORRESPONDÊNCIA

Proposição 1. (1º Teorema do Isomorfismo de Anéis). Se $\psi: A \longrightarrow A'$ é um homomorfismo sobrejetivo de anéis e $I = Ker\, \psi$, então os anéis $A/_I$ e A' são isomorfos. Precisamente, a aplicação $\overline{\psi}: A/_I \longrightarrow A'$ dada por $\overline{\psi}(a + I) = \psi(a)$ é um isomorfismo.
Demonstração. Notemos inicialmente que se $a \equiv b(mod\, I)$, ou seja, se $a + I = b + I$ então $a - b \in I$ e $\psi(a - b) = 0$ donde temos que $\psi(a) = \psi(b)$. Logo, $\overline{\psi}$ está bem definida. Como, $\overline{\psi}\big((a + I) + (b + I)\big) = \overline{\psi}\big((a + b) + I\big) = \psi(a + b) = \psi(a) + \psi(b) = \overline{\psi}(a + I) +$
$\overline{\psi}(b + I)$e

$\overline{\psi}\big((a+I)+(b+I)\big)=\overline{\psi}(ab+I)=\psi(ab)=\psi(a)\cdot\psi(b)=\overline{\psi}(a+I)\cdot\overline{\psi}(b+I)$, logo, $\overline{\psi}$ é um homomorfismo.

Finalmente, $a+I\in Ker\,\overline{\psi}\Leftrightarrow\overline{\psi}(a+I)=0\Leftrightarrow\psi(a)=0\Leftrightarrow a\in Ker\,\psi=\{I\}$ ou seja, $\overline{\psi}$ é injetiva. Como $Im\,\overline{\psi}=Im\,\psi$ segue que:

$\overline{\psi}: {}^{A}/_{I}\longrightarrow A'$ é um isomorfismo de anéis.

Escrevemos: ${}^{A}/_{I}\approx A'$.

Exemplo 1. Dados dois anéis *A* e *B* definimos o produto direto dos anéis *A* e *B* como sendo o anel $A\times B=\{(a,b);\ a\in A \text{ e } b\in B\}$ no qual estão definidas as operações dadas $(a,b),(a',b')\in A\times B$, $(a,b)+(a',b')=(a+b,a'+b')$ e $(a,b)\cdot(a',b')=(aa',bb')$. O zero deste anel é $(0,0)$. Quando $A=m\mathbb{Z}$ e $B=n\mathbb{Z}$, com $m,n\in\{2,3,4,\dots\}$ e $mdc(m,n)=1$, a aplicação $\psi:\mathbb{Z}\longrightarrow\left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\times{}^{\mathbb{Z}}/_{n\mathbb{Z}}\right)$, dada por $\psi(a)=(a+m\mathbb{Z},a+n\mathbb{Z})$ é sobrejetiva e tem núcleo $mn\mathbb{Z}$. Do primeiro teorema dos isomorfismos segue que

$$\frac{\mathbb{Z}}{mn\mathbb{Z}}\approx\frac{\mathbb{Z}}{m\mathbb{Z}}\times\frac{\mathbb{Z}}{n\mathbb{Z}}$$

Vamos às contas!

Afirmação. ψ é um homomorfismo.

De fato, dados $a,b\in\ \mathbb{Z}$,

$\psi(a+b)=\big((a+b)m\mathbb{Z},(a+b)n\mathbb{Z}\big)$

$=\big((a+m\mathbb{Z})+(b+m\mathbb{Z}),(a+n\mathbb{Z})+(b+n\mathbb{Z})\big)$

$=(a+m\mathbb{Z},a+n\mathbb{Z})+(b+m\mathbb{Z},b+n\mathbb{Z})$

$=\ \psi(a)+\psi(b)$

Analogamente, $\psi(a\cdot b)=(ab+m\mathbb{Z},ab+n\mathbb{Z})=(a+m\mathbb{Z},a+n\mathbb{Z})\cdot(b+m\mathbb{Z},b+n\mathbb{Z})=\psi(a)\cdot\psi(b)$.

Afirmação. $Ker\,\psi=mn\mathbb{Z}$.

Seja $a\in\mathbb{Z}$ e suponhamos que $\psi(a)=(m\mathbb{Z},n\mathbb{Z})$. Ou seja, $a+m\mathbb{Z}=m\mathbb{Z}$ e $a+n\mathbb{Z}=n\mathbb{Z}$. Segue que $a\in m\mathbb{Z}\cap n\mathbb{Z}$, ou seja, $m,n|a$. Como $mdc(m,n)=1$, temos que $mn|a$ isto é, $a\in mn\mathbb{Z}$. Se $a\in mn\mathbb{Z}$ então $m|a$ e $n|a$ donde temos que $a\in m\mathbb{Z}$ e $a\in n\mathbb{Z}$ de modo que $\psi(a)=(a+m\mathbb{Z},a+n\mathbb{Z})=(m\mathbb{Z},n\mathbb{Z})$ ou seja, $Ker\,\psi=mn\mathbb{Z}$.

Afirmação.(Teorema chinês dos restos). A aplicação ψ é sobrejetiva. De fato $(a+m\mathbb{Z},b+n\mathbb{Z})\in\frac{\mathbb{Z}}{m\mathbb{Z}}\times\frac{\mathbb{Z}}{n\mathbb{Z}}$, como $mdc(m,n)=1$ existe um $c\in\mathbb{Z}$ tal que $c\equiv a(mod\,m)$, portanto $c+m\mathbb{Z}=a+m\mathbb{Z}$ e $c+n\mathbb{Z}=b+n\mathbb{Z}$ de modo que $\psi(c)=(c+m\mathbb{Z},c+n\mathbb{Z})=(a+m\mathbb{Z},b+m\mathbb{Z})$.

Notemos que, sendo $mdc(m,n)=1$, existem $r,s\in\mathbb{Z}$ tais que $mr+ms=1$. Tome c como sendo $c=ans+bmr$ então:

$c\equiv ans(mod\,m)$ e como $ns\equiv 1(mod\,m)$ segue que $c\equiv a(mod\,m)$

$c\equiv bmr(mod\,n)$ e como $mr\equiv 1(mod\,n)$ temos que $c\equiv b(mod\,n)$.

Proposição 2. (2º teorema dos isomorfismos de anéis). Sejam A um anel, I um ideal de A e B um subanel de A. Então $I + B = \{a + b; a \in I, b \in B\}$ é um subanel de A, I é um ideal de $I + B, I \cap B$ é um ideal de B e vale:

$$\frac{I+B}{I} \approx \frac{B}{I \cap B}$$

Demonstração. Vamos mostrar apenas o isomorfismo. Com efeito, consideremos a aplicação $\psi: B \longrightarrow \frac{I+B}{I}$ dada por $\psi(b) = b + I$. Então, $\psi(b_1 + b_2) = (b_1 + b_2) + I = (b_1 + I) + (b_2 + I) = \psi(b_1) + \psi(b_2)$.

Analogamente, $\psi(b_1 \cdot b_2) = (b_1 \cdot b_2) + I = (b_1 + I) \cdot (b_2 + I) = \psi(b_1) \cdot \psi(b_2)$ ou seja, ψ é um homomorfismo.

Agora, $b \in Ker\ \psi \Leftrightarrow \psi(b) = b + I = I \Leftrightarrow b \in I$. Logo, $Ker\ \psi = I \cap B$.

Finalmente, dado $a + b \in I + B$ com $a \in I$ e $b \in B$, notemos que $(a + b) + I = b + I$, pois $a \in I$. Assim, $\psi(b) = b + I = (a + b) + I$, ou seja, ψ é sobrejetiva. Segue do 1º teorema dos isomorfismos que

$\frac{B}{I \cap B} \approx \frac{I+B}{I}$, como queríamos demonstrar.

Proposição 3. (3º teorema dos isomorfismos para anéis). Sejam A uma anel, I e J ideais de A com $I \subset J$. Então I é um ideal de J, ${}^{J}/_{I}$ é um ideal de ${}^{A}/_{I}$ e temos o isomorfismo de anéis.

$$\frac{{}^{A}/_{I}}{{}^{J}/_{I}} \approx {}^{A}/_{J}.$$

Demonstração. Demonstraremos apenas o isomorfismo. Consideremos a aplicação:

$\psi: \frac{A\prime}{I} \longrightarrow \frac{A}{J}$ dada por $\psi(a + I) = a + J$. É fácil ver que ψ é um homomorfismo. Seja $a + I \in Ker\ \psi \Leftrightarrow \psi(a + I) = a + J = J \Leftrightarrow a + J$.

Logo, $Ker\ \psi = \{a + I; a \in J\} = \frac{J}{I}$.

Dado $a + J \in {}^{A}/_{J}$, temos que $\psi(a + I) = a + J$, ou seja, ψ é sobrejetiva. Logo, do 1º teorema, segue que $\frac{{}^{A}/_{I}}{{}^{A}/_{J}} \approx {}^{A}/_{J}$, como queríamos demonstrar.

Observação. Caro aluno, os dois últimos teoremas têm valor teórico, podem ser utilizados em cursos futuros e nós queremos apenas que você olhe para eles, neste momento, como exemplos de aplicações do primeiro teorema.

Proposição 4. (Teorema da correspondência). Seja $\psi: A \longrightarrow A'$ um homomorfismo sobrejetivo de anéis. Existe uma bijeção entre ideais de A contendo $Ker\ \psi$ e ideais de A' dada por $I \longleftrightarrow \psi(I)$.

Demonstração. Primeiro, notemos que como ψ é sobrejetiva, para cada ideal I de A, $\psi(I)$ é um ideal de A'. Para ver isto, $\psi(0) = 0 \Longrightarrow 0 \in \psi(I)$. Se $a', b' \in \psi(I)$, existem $a, b \in I$ tais que $\psi(a) = a'$ e $\psi(b) = b'$ de modo que $\psi(a - b) = a' - b'$ e como $a - b \in I$, segue que $a' - b' \in \psi(I)$.

Dados $a' \in A'$ e $b' \in \psi(I)$ existem $a \in A$ e $b \in I$ tais que $\psi(ab) = a' \cdot b'$ e como $ab \in I, a' \cdot b' \in \psi(I)$, ou seja, $\psi(I)$ é um ideal de A'.

Agora, sejam I um ideal de A contendo $Ker\, \psi, b \in I$ e $a \in A$ tais que $\psi(a) = \psi(b) \in \psi(I)$. Então $\psi(b - a) = 0$ isto é, $b - a \in Ker\, \psi \subset I \Longrightarrow b \in a + I = I$, ou seja, a correspondência $I \longrightarrow \psi(I)$ é injetiva.

Dado $J \in A'$, o conjunto $I = \psi^{-1}\,(J)$ é um ideal de A, pois, dados $a, b \in I, \psi(a),\ \psi(b) \in J \Longrightarrow \psi(a) - \psi(b) = \psi(a - b) \in J \Longrightarrow a - 1 \in \psi^{-1}(J) = I.$

Se a $\in A$ e $b \in I$ então $\psi(ab) = \psi(a) \cdot \psi(b)$ e como $\psi(b) \in J$ segue que $\psi(ab) \in J$ e consequentemente $ab \in \psi^{-1}(J) = I.$

Logo $I = \psi^{-1}(J)$ é tal que $\psi(I) = J$ donde temos que a correspondência $I \longleftrightarrow \psi(I)$ entre ideais de A contendo $Ker\, \psi$ e suas imagens diretas em A' é uma bijeção.

RESUMO

Nesta aula começamos definindo, exemplificando e classificando os homomorfismos de anéis. Definimos núcleo e imagem destes homomorfismos e, em seguida estabelecemos os seus teoremas clássicos, os três de isomorfismos e o da correspondência que são ferramentas básicas para cursos de Álgebra posteriores.

ATIVIDADES

1. Prove que o único automorfismo de $\mathbb{Q}$ é a identidade $(Aut\ \mathbb{Q} = \{I\mathbb{Q}\})$.
2. Prove que os subcorpos de $\mathbb{R}$, $\mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ e $\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3}; a, b \in \mathbb{Q}\}$ não são isomorfos.
3. Sejam A e B anéis e sejam $\psi_1 : A \times B \longrightarrow A$ e $\psi_2 : A \times B \longrightarrow B$ dadas por $\psi_1(a, b) = a$ e $\psi_2(a, b) = b$. Prove que ambas são homomorfismos sobrejetivos (epimorfismos). Calcule $N_1 = Ker\, \psi_1, N_2 = Ker\, \psi_2$ e conclua que $\frac{A \times B}{N_1} \approx A$ e $\frac{A \times B}{N_2} \approx B$.
4. Sejam m e n inteiros positivos coprimos e Φ a função Phi de Euller. Prove que $\Phi(mn) = \Phi(m) \cdot \Phi(n)$.
5. Sejam A e A' anéis comutativos com identidades e $\psi: A \longrightarrow A'$ um homomorfismo sobrejetivo. Prove que $I \subset A$ é um ideal primo se, e somente se $\psi(I)$ é primo.

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade, você deve ter usado o exemplo 4, para concluir que $\psi(a) = a, \forall a \in \mathbb{Z}$ e notado que para cada $a > 1, a^{-1} \cdot a = 1 \Longrightarrow \psi(a^{-1}) = \psi(a)^{-1}$.

Na segunda atividade, você deve ter notado que se existisse um isomorfismo $\psi: \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{3}]$ então, por ser $\psi(\sqrt{2}) = \pm\sqrt{2}$ teríamos $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$ o que não é verdade.

Na terceira atividade, você deve ter usado as respectivas definições e o 1º teorema dos isomorfismos.

Se você conseguiu fazer a quarta atividade, deve ter usado o exemplo 4 e a definição da função Phi de Euller.

Notemos que na quinta atividade estamos afirmando que no teorema da correspondência, o correspondente de um ideal primo é também um ideal primo. Para provar este resultado, você deve ter apenas usado com cuidado a definição de ideal primo.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).